AMENDMENTS TO THE CLAIMS

Claim 1. (currently amended) A digital data delivery method for use in delivering digital data from an upstream system to a downstream system, said upstream system providing multipoint delivery of encrypted digital data to specific destinations, and said downstream system decrypting the delivered digital data, said method comprising the steps of:

encrypting digital data by said upstream system using an encryption key;

generating a plurality of pieces of key information on the basis of said encryption key, respective pieces of said key information being generated by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

delivering said respective pieces of key information to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other;

delivering the encrypted digital data;

restoring said encryption key by said downstream system using said respective pieces of key information delivered over said plurality of delivery routes; and

using the restored encryption key to decrypt the encrypted digital data.

Claim 2. (currently amended) A digital data delivery method for use in delivering digital data from an upstream system to a downstream system, said upstream system providing multipoint delivery of encrypted digital data to specific destinations, and said downstream system decrypting the delivered digital data, said method comprising the steps of:

encrypting digital data by said upstream system using an encryption key;

generating on the basis of said encryption key, sets of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

delivering either a set of passkeys or passkey information, from which said passkeys may be reproduced, to a respective destination over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other;

delivering the encrypted digital data;

restoring said encryption key by said downstream system using either said set of passkeys or said passkey information delivered over said plurality of delivery routes; and

using the restored encryption key to decrypt the encrypted digital data.

Claim 3. (currently amended) A digital data delivery method for use in delivering digital data from an upstream system to a downstream system, said upstream system providing multipoint delivery of encrypted digital data to specific destinations, and said downstream system decrypting the delivered digital data, said method comprising the steps of:

encrypting digital data by said upstream system using an encryption key;

generating on the basis of said encryption key, a set of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced;

delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information, to each of said specific destinations over

a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other;

delivering the encrypted digital data;

restoring said encryption key by using said downstream system using either said plurality of partial keys or said partial key information and using either said remaining passkeys or said remaining passkey information delivered over said plurality of delivery routes; and

using the restored encryption key to decrypt the encrypted digital data.

Claim 4. (canceled)

Claim 5. (currently amended) A digital data delivery method for use in delivering digital data from an upstream system to a downstream system, said upstream system providing multipoint delivery of encrypted digital data to specific destinations, and said downstream system decrypting the delivered digital data, said method comprising the steps of:

encrypting digital data by said upstream system using a first encryption key;

generating a second encryption key specific to each of said specific destinations and/or to said digital data;

using said second encryption key to encrypt either said first encryption key or first encryption key information from which said first encryption key may be reproduced;

generating, on the basis of said second encryption key, a set of passkeys by dividing said encryption key by a division pattern unique to each of said specific destinations;

delivering either said encrypted first encryption key or said encrypted first encryption key information and delivering either said set of passkeys or passkey information,

from which said set of passkeys may be reproduced, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other;

delivering the encrypted digital data;

restoring said second encryption key by using either said set of passkeys or said passkey information delivered over said plurality of delivery routes so as to decrypt either said first encryption key or said first encryption key information and thereby restore said first encryption key; and

decrypting the encrypted digital data by use of the restored first encryption key.

Claim 6. (currently amended) A signal processing method for use with an upstream system providing multipoint delivery of encrypted digital data to specific destinations, said method comprising the steps of:

encrypting digital data by said upstream system using an encryption key;

generating a plurality of pieces of key information, on the basis of said encryption key, respective pieces of said key information being generated by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

delivering said respective pieces of key information to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

delivering the encrypted digital data.

Claim 7. (currently amended) A signal processing method for use with an upstream system providing multipoint delivery of encrypted digital data to specific destinations, said method comprising the steps of:

encrypting digital data by said upstream system using an encryption key;

generating on the basis of said encryption key, sets of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to said specific destinations;

delivering either a set of passkeys or passkey information, from which said passkeys may be reproduced, to a respective destination over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

delivering the encrypted digital data.

Claim 8. (currently amended) A signal processing method for use with an upstream system providing multipoint delivery of encrypted digital data to specific destinations, said method comprising the steps of:

encrypting digital data by said upstream system using an encryption key;

generating on the basis of said encryption key, a set of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced;

delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information, to each of said specific destinations over

a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

delivering the encrypted digital data.

Claim 9. (canceled)

Claim 10. (currently amended) A signal processing method for use with an upstream system providing multipoint delivery of encrypted digital data to specific destinations, said method comprising the steps of:

encrypting digital data by said upstream system using a first encryption key;

generating a second encryption key specific to each of said specific destinations and/or to said digital data;

using said second encryption key to encrypt either said first encryption key or first encryption key information from which said first encryption key may be reproduced;

generating, on the basis of said second encryption key, a set of passkeys by dividing said encryption key by a division pattern unique to each of said specific destinations;

delivering either said encrypted first encryption key or said encrypted first encryption key information and delivering either said set of passkeys or passkey information, from which said set of passkeys may be reproduced, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

delivering the encrypted digital data.

Claim 11. (currently amended) A digital data delivery system comprising an upstream system providing multipoint delivery of encrypted digital data to specific destinations and a downstream system decrypting the delivered digital data;

said upstream system including:

an encrypting element for encrypting digital data using an encryption key;

a key information generator for generating a plurality of pieces of key information on the basis of said encryption key, respective pieces of said key information being generated by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

a key information delivery element for delivering said respective pieces of key information to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from one another; and

a digital data delivery element for delivering the encrypted digital data;

and said downstream system including:

an encryption key restoring element for restoring said encryption key using respective pieces of key information delivered over said plurality of delivery routes; and

a decrypting element for decrypting the encrypted digital data by using the restored encryption key.

Claim 12. (currently amended) A digital data delivery system comprising an upstream system providing multipoint delivery of encrypted digital data to specific destinations and a downstream system decrypting the delivered digital data;

said upstream system including:

an encrypting element for encrypting digital data using an encryption key;

a key information generator for generating, on the basis of said encryption key, sets of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to said specific destinations;

a key information delivery element for delivering either a set of passkeys or passkey information, from which said passkeys may be reproduced, to a respective destination over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

a digital data delivery element for delivering the encrypted digital data;

and said downstream system including:

an encryption key restoring element for restoring said encryption key using either said set of passkeys or said passkey information delivered over said plurality of delivery routes; and

a decrypting element for decrypting the encrypted digital data using the restored encryption key.

Claim 13. (currently amended) A digital data delivery system comprising an upstream system providing multipoint delivery of encrypted digital data to specific destinations and a downstream system decrypting the delivered digital data;

said upstream system including:

an encrypting element for encrypting digital data using an encryption key;

a first key information generator for generating, on the basis of said encryption key, a set of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

a second key information generator for generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information, from which said passkeys may be reproduced;

a key information delivery element for delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and for delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

a digital data delivery element for delivering the encrypted digital data;

and said downstream system including:

an encryption key restoring element for restoring said encryption key using either said plurality of partial keys or said partial key information and using either said remaining passkeys or said remaining passkey information delivered over said plurality of delivery routes; and

a decrypting element for decrypting the encrypted digital data using the restored encryption key.

Claim 14. (canceled)

Claim 15. (currently amended) A digital data delivery system comprising an upstream system providing multipoint delivery of encrypted digital data to specific destinations and a downstream system decrypting the delivered digital data;

said upstream system including:

an encrypting element for encrypting digital data using a first encryption key;

an encryption key generator for generating a second encryption key specific to each of said specific destinations and/or to said digital data;

a first key information generator using said second encryption key for encrypting either said first encryption key or first encryption key information from which said first encryption key may be reproduced;

a second key information generator using said second encryption key for generating a set of passkeys by dividing said encryption key by a division pattern unique to each of said specific destinations;

a key information delivery element for delivering either said encrypted first encryption key or said encrypted first encryption key information and for delivering either said set of passkeys or passkey information from which said set of passkeys may be reproduced, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

a digital data delivery element for delivering the encrypted digital data;

and said downstream system including:

an encryption key restoring element for restoring said second encryption using either said set of passkeys or said passkey information delivered over said plurality of delivery routes

so as to decrypt either said first encryption key or said first encryption key information and thereby restore said first encryption key; and

a decrypting element for decrypting the encrypted digital data by use of the restored first encryption key.

Claim 16. (currently amended) An upstream system for providing multipoint delivery of encrypted digital data to specific destinations, comprising:

an encrypting element for encrypting digital data using an encryption key;

a key information generator for generating a plurality of pieces of key information, on the basis of said encryption key, respective pieces of said key information being generated by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

a key information delivery element for delivering said respective pieces of key information to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

a digital data delivery element for delivering the encrypted digital data.

Claim 17. (currently amended) An upstream system for providing multipoint delivery of encrypted digital data to specific destinations, comprising:

a key information generator for generating, on the basis of said encryption key, sets of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

a key information delivery element for delivering either said set of passkeys or passkey information, from which said passkeys may be reproduced, to a respective destination over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

a digital data delivery element for delivering the encrypted digital data.

Claim 18. (currently amended) An upstream system for providing multipoint delivery of encrypted digital data to specific destinations, comprising:

an encrypting element for encrypting digital data using an encryption key;

a first generator for generating on the basis of said encryption key, a set of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

a second generator for generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced;

a key information delivery element for delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

a digital data delivery element for delivering the encrypted digital data.

Claim 19. (canceled)

Claim 20. (currently amended) An upstream system for providing multipoint delivery of encrypted digital data to specific destinations, comprising:

a first encrypting element for encrypting digital data using a first encryption key;

a first generator for generating a second encryption key specific to each of said specific destinations and/or to said digital data;

a second encrypting element using said second encryption key to encrypt either said first encryption key or first encryption key information from which said first encryption key may be reproduced;

a second generator for generating, on the basis of said second encryption key, a set of passkeys by dividing said encryption key by a division pattern unique to each of said specific destinations;

a key information delivery element for delivering either said encrypted first encryption key or said encrypted first encryption key information and for delivering either said set of passkeys or passkey information, from which said set of passkeys may be reproduced, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

a digital data delivery element for delivering the encrypted digital data.

Claim 21. (currently amended) A storage medium which stores a computer-readable program for controlling the steps of:

encrypting digital data using an encryption key;

generating a plurality of pieces of key information, on the basis of said encryption key, respective pieces of said key information being generated by dividing said encryption key by a division pattern unique ~~specific~~ to each of specific destinations;

delivering said respective pieces of key information to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

performing multipoint delivery of the encrypted digital data to said specific destinations.

Claim 22. (currently amended) A storage medium which stores a computer-readable program for controlling the steps of:

encrypting digital data using an encryption key;

generating on the basis of said encryption key, sets of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to each of said specific destinations;

delivering either a set of passkeys or passkey information, from which said passkeys may be reproduced, to a respective destination over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

performing multipoint delivery of the encrypted digital data to said specific destinations.

Claim 23. (currently amended) A storage medium which stores a computer-readable program for controlling the steps of:

encrypting digital data using an encryption key;

generating on the basis of said encryption key, a set of passkeys by dividing said encryption key by a division pattern unique ~~specific~~ to each of specific destinations;

generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced;

delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

performing multipoint delivery of the encrypted digital data to said specific destinations.

Claim 24. (canceled)

Claim 25. (currently amended) A storage medium which stores a computer-readable program for controlling the steps of:

encrypting digital data by said upstream system using a first encryption key;

generating a second encryption key specific to each of said specific destinations and/or to said digital data;

using said second encryption key to encrypt either said first encryption key or first encryption key information from which said first encryption key may be reproduced;

generating, on the basis of said second encryption key, a set of passkeys by dividing said encryption key by a division pattern unique to each of said specific destinations;

delivering either said encrypted first encryption key or said encrypted first encryption key information and delivering either said set of passkeys or passkey information, from which said set of passkeys may be reproduced, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; and

performing multipoint delivery of the encrypted digital data to said specific destinations.